INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG2004/000320

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. [7]: H04L 9/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WPAT, USPTO: CRYPTOGRAPHIC, KEY, PRIVATE, SPLIT AND SIMILAR TERMS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2000/049768 A1 (MITTELHOLZER) 24 August 2000 Whole document	1-19
X	US 2002/0076042 A1 (SANDHU et al.) 20 June 2002 Whole document	15, 16, 19
X	US 5905799 A (GANESAN) 18 May 1999 Whole document	15, 16, 19

☐ Further documents are listed in the continuation of Box C ☒ See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 November 2004	22 NOV 2004
Name and mailing address of the ISA/AU	Authorized officer
AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	**SUSHIL AGGARWAL** Telephone No : (02) 6283 2192

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG2004/000320

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a)

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:
See extra sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☒ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG2004/000320

Supplemental Box
(To be used when the space in any of Boxes I to VIII is not sufficient)

Continuation of Box No:

The international application does not comply with the requirements of unity of invention because it does not relate to one invention or to a group of inventions so linked to form a single general inventive concept. In coming to this conclusion, the International Searching Authority has found that there are different inventions as follows:

1. Claims 1-14, 17 and 18 relate to cryptographically processing a message wherein the message is processed using a first partial cryptographic key corresponding to a decomposition of a private key, resulting in a first partially processed message, the message is processed using a second partial cryptographic key corresponding to the decomposition of the private key, resulting in a second partially processed message, the first partially processed message and the second partially processed message are combined resulting in a cryptographically processed message.

2. Claims 15, 16 and 19 relate to cryptographically processing a message wherein the message is processed using a partial cryptographic key corresponding to a decomposition of a private key, resulting in a partially processed message.

The above groups of inventions are no so linked as to form a single general inventive concept, that is, they do not have any common inventive features, which defines a contribution over the prior art. The common concept linking together these groups of claims is processing a message using a partial cryptographic key corresponding to a decomposition of a private key. However this concept is not novel in the light of any of the following documents:

D1: WO 2000/049768 A1 (MITTELHOLZER) 24 August 2000
D2: US 2002/0076042 A1 (SANDHU et al.) 20 June 2002
D3: US 5905799 A (GANESAN) 18 May 1999

Consequently the common feature does not constitute a 'special technical feature' within the meaning of PCT Rule 13.2 since it makes no contribution over the prior art. Therefore, these claims lack unity, a posteriori.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/SG2004/000320

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member	
WO	2000/049768	NONE	
US	2002/0076042	WO	2002/051062
US	5905799	US	5588061

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

END OF ANNEX